REMARKS

Claims **107-147** and **165-181** are pending in the application.

Claims **107-147** and **165-181** stand rejected.

Claims **107, 111-115, 117-118, 120, 126-128, 131, 134-140, 146-147, 165, 169-174, 176, 178** and **180-181** have been amended.

Claims **1-106, 108-109, 123, 125, 132-133, 143, 145, 148-164, 166-167, 177** and **179** have been cancelled.

Formal Matters

Claim 131 stands objected to because of an informality. Claim 131 has been amended to correct the informality.

Rejection of Claims under 35 U.S.C. §101

Claims 165 and 174 stand rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Applicants have amended claims 165 and 174 to address the Examiner's concerns by affirmatively reciting computer readable storage media as an element of the claimed computer program product. Applicants therefore respectfully submit that this rejection is overcome thereby.

Rejection of Claims Under 35 U.S.C. §103

Claims 107-115, 131-139 and 165-173 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,064,671 issued to Killian ("Killian") in view of U.S. Patent No. 6,643,701 issued to Aziz et al. ("Aziz").

Claims 116-119 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,064,671 issued to Killian ("Killian") in view of U.S. Patent No. 6,643,701 issued to Aziz et al. ("Aziz"), in further view of U.S. Patent No. 6,104,716 issued to Crichton et al. ("Crichton").

Claims 120-124, 128-130, 140-144 and 174-178 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,643,701 issued to Aziz et al. ("Aziz"), in further view of U.S. Patent No. 6,104,716 issued to Crichton et al. ("Crichton").

Claims 125-127, 145-147 and 179-181 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,643,701 issued to Aziz et al. ("Aziz") in view of U.S. Patent No. 6,104,716 issued to Crichton et al. ("Crichton") and further in view of U.S. Patent No. 6,064,671 issued to Killian ("Killian").

As an initial matter, Applicants respectfully submit that the rejection of claims 108-109, 123, 125, 132-133, 143, 145, 166-167, 177 and 179 is moot, as these claims have been cancelled. However, the limitations of these claims have been amended into their respective independent claims (claims 107, 120, 131, 140, 165 and 174), among other amendments. Applicants therefore respectfully submit that the rejection of claims 120 and 140, and those of claims depending thereon, for at least the reason that the Office Action fails to show the manner in

which the cited references might be combined to make obvious the limitations now recited in amended independent claims 120 and 140, in addition to the reasons set forth subsequently.

While not conceding that the cited references qualify as prior art, but instead to expedite prosecution, Applicants have chosen to respectfully disagree and traverse the rejection as follows. Applicants reserve the right, for example, in a continuing application, to establish that the cited references, or other references cited now or hereafter, do not qualify as prior art as to an invention embodiment previously, currently, or subsequently claimed.

In order for a claim to be rendered invalid under 35 U.S.C. § 103, the subject matter of the claim as a whole would have to be obvious to a person of ordinary skill in the art at the time the invention was made. *See* 35 U.S.C. § 103(a). This requires: (1) the reference(s) must teach or suggest all of the claim limitations; (2) there must be some teaching, suggestion or motivation to combine references either in the references themselves or in the knowledge of the art; and (3) there must be a reasonable expectation of success. *See* MPEP 2143; MPEP 2143.03; *In re Rouffet*, 149 F.3d 1350, 1355-56 (Fed. Cir. 1998).

In this regard, independent claim 107, as amended, now recites:

107. A method comprising:
providing a plurality of sockets, wherein
each socket has an associated connection and an associated security token,
each associated connection is inbound relative to a relay program, and
the associated security token is provided by the associated connection;
receiving a first connection and a first security token at a relay program, wherein
the first connection is inbound relative to the relay program;
creating a socket associated with the first connection, wherein

the creating comprises associating the first security token with the first connection;

comparing the first security token with the associated security tokens; and

in response to said comparing,

if none of the associated security tokens match the first security token, including the socket in the plurality of sockets, and

if the first security token and a security token associated with one of the plurality of sockets match, coupling an end point of the first connection to an end point of a connection associated with the socket associated with the matching security token, wherein

a security token is a password, and

the connection associated with the socket is inbound relative to the relay program.

Independent claim 120 has also been amended, and now recites:

120. A method comprising:

creating a first connection from a first program to a relay program, wherein the first connection is inbound to the relay program;

receiving a first security token from the first program at the relay program, wherein the first security token is a password;

providing the first security token to the relay program;

creating a socket associated with the first connection, wherein

the creating comprises associating the first security token with the first connection;

comparing the first security token with one or more security tokens associated with one or more corresponding connections, wherein

each one of the one or more corresponding connections is inbound to the relay program; and

in response to said comparing,

if the first security token and a security token associated with a corresponding connection match,

coupling the second connection to the connection associated with the matching security token, and

if none of the associated security tokens match the first security token,

creating a second connection to the relay program, wherein the second connection is inbound to the relay program,

upon successful creation of the second connection,

including the second connection with said one or more corresponding connections, and

coupling the first connection and the second connection to one another

As will be appreciated, amended independent claims 131, 140, 165 and 174 recite, at least in part, substantially comparable limitations.

By contrast to the foregoing, Killian, which is concerned with a multi-homed end system for increasing computers' network bandwidth, discloses:

> "Network computers have a plurality of network-level interfaces associated with overlapping portions of the network-level address space, such as those represented by multiple static entries with the same address range, or multiple default entries in a network-level routing table. The computers distribute outgoing messages address [*sic*] to the overlapping portions of the address space between the multiple network interfaces associated with those overlapping portions. In the TCP/IP environment, the distribution of messages can be

performed on the basis of the outgoing message's source port, the amount of traffic associated with a TCP/IP service indicated by the message's destination port, or by the relative amount of traffic going though each of the respective network interfaces. In some embodiments, the computers are multi-homed end systems which pick the source address of outgoing messages and their associated socket. In some embodiments, the network interfaces between which messages are distributed are dial-up modems having network-level addresses dynamically allocated to them by the computer to which they are connected. Some systems can automatically connect or disconnect such dial-up connections in response to changes communications demands. In some embodiments of the invention, a multi-homed end system distributes messages addressed to a given destination address between multiple network interfaces for the purpose of load testing." (Killian, Abstract)

By contrast to the foregoing, Aziz, which is concerned with providing secure communication with a relay in a network, discloses:

"Methods and systems of the present invention include providing a connection between a first computer and a second computer by receiving, at a third computer, information regarding one of the first and second computers to facilitate establishment of a secure connection between the first computer and the second computer, creating a first end-to-end security link between the first computer and third computer, and creating a second end-to-end security link

between the second computer and the third computer to establish the secure connection. The first and second computers could be a client and a server on the Internet, and these methods and systems can, for example, increase the possible number of new secure connections to the server. The third computer also permits processing of information transmitted between the client and server in the third computer. For example, the information could be reformatted or used in testing a process of one of the first and second computers." (Aziz, Abstract)

As will be noted, Killian and Aziz, taken alone or in any permissible combination, fail to show, teach or suggest, a system in which the use of a security token that is a password, particularly when that security token is used in creating a socket associated with a first connection, in which the creation of the first connection includes associating the first security token with the first connection. Applicants respectfully submit that the Office Action does not establish the presence of these limitations in Killian and Aziz, taken alone or in any permissible combination.

As an initial matter, Applicants respectfully note that the association between a first security token that is a password and a first connection is not specifically addressed in the Office Action. To underscore and more clearly delineate this distinction, Applicants have amended independent claims 107, 120, 131, 140, 165 and 174 to specifically recite the use of a password in this association. Support for this association and related amendments can be found at least, for example, at operation 400 of Figure 4 and p. 11, lines 19 through p. 12, line 15 of the Specification; and other description associated with Figure 4. Moreover, support for the security

token being a password can be found throughout the Detailed Description of the Invention in the present Specification. Thus, no new matter is added thereby.

As an initial matter, Applicants once again note that the Office Action appears to draw a parallel between a network address and a security token that is a password, which Applicants respectfully submit is inapposite. Furthermore, a network address is not a security token that is a password for the simple fact that a network address does not serve to secure anything, nor is a network address a password in any respect. A security token that is a password is one or more units of information that can be used for authorization, authentication and access.

Furthermore, even if a parallel could successfully be maintained between a network address and a security token that is a password (which Applicants maintain is not an appropriate parallel to be drawn from the cited references), nowhere in Killian or Aziz is there shown, taught or suggested an act or apparatus for associating a first security token that is a password and a first connection. Aside from the cited references failing to show, teach or suggest a first security token, the actual association of a first security token and a first connection is not shown, taught or suggested by Killian and Aziz, taken alone or in any permissible combination, in any event. As will be appreciated, lacking a teaching of a security token that is a password, no such act or apparatus regarding such a feature would be expected to be taught thereby.

Unfortunately, Aziz fails to cure the aforementioned infirmities, as well as the infirmity for which Aziz is cited in the Office Action. First, the logical inconsistencies to which the citations to which Killian fall prey could not be solved by any reference. Moreover, not only is Aziz not cited in regard to the claimed security token that is a password, there is no showing, teaching or suggestion In the Office Action (or otherwise), that Aziz could provide such teachings, and in fact, Aziz does not. Crichton, cited against the limitations of certain claims

now recited in the amended independent claims, also fails to provide any such solution, failing to show, teach or suggest anything comparable to the claimed password, even if such features were taken only by themselves (which Applicants maintain is inapposite, given that all the features are cited against the same limitation).

By contrast to the foregoing, Crichton, which is concerned with lightweight secure communication tunneling over the internet, discloses:

> "A lightweight secure tunneling protocol or LSTP permits communicating across one or more firewalls by using a middle server or proxy. Three proxies are used to establish an end-to-end connection that navigates through the firewalls. In a typical configuration, a server is behind a first firewall and a client behind a second firewall are interconnected by an untrusted network (e.g., the Internet) between the firewalls. A first inside firewall SOCKS-aware server-side end proxy connects to the server inside the first firewall. A second inside firewall SOCKS-aware client-side end proxy is connected to by the client inside the second firewall. Both server-side and client-side end proxies can address a third proxy (called a middle proxy) outside the two firewalls. The middle proxy is usually started first, as the other two end proxies (server and client) will initiate the connection to the middle proxy some time after they are started. Since the middle proxy is mutually addressable by both inside proxies, a complete end-to-end connection between the server and client is established. It is the use of one or more middle proxies together with the LSTP that establishes the secure communications link or tunnel across multiple firewalls." (Crichton, Abstract)

Applicants do not see that Crichton provides any meaningful supplement to Killian or Aziz, and, in fact, fails to inform any argument as to the purported obviousness of the claims in question. The use of a virtual private network (VPN) through a firewall using known techniques is not material to either the purported combination of Killian and Aziz, or the claimed invention. Applicants fail to appreciate how Crichton differs meaningfully from Aziz, and so are left to question why one of skill in the art would find any reason to look to what is fundamentally a cumulative source of information to Aziz.

The Office Action thus fails to establish the presence of the foregoing limitations in Killian, Aziz and Crichton, taken alone or in permissible combination. As will be appreciated, the Office Action bears the burden of supporting a case of obviousness, including whether the prior art references teach or suggest all of the claim limitations. *See* MPEP 706.02(j). For at least the foregoing reasons, neither Killian nor Aziz, alone or in combination (even in view of Crichton), shows, teaches or suggests such limitations.

With regard to the motivation to combine the references, Applicants respectfully submit that each of Killian and Aziz (as well as Crichton) provide complete, self-contained solutions to the issues each addresses. Thus, as will be appreciated, Killian is directed to a multi-homed end system for increasing computers' network bandwidth. To accomplish this end, a system according to Killian employs network computers having a plurality of network-level interfaces associated with overlapping portions of the network-level address space. By doing so, Killian's network computers distribute outgoing messages to the overlapping portions of the address space between the multiple network interfaces associated with those overlapping portions. As will be

appreciated, then, Killian already provides for communication between computers on a network, in a situation in which multiple computers are to receive the same outgoing messages.

By contrast, Aziz is directed to providing secure communication with a relay in a network. Aziz accomplishes this by providing a connection between a first computer and a second computer by receiving, at a third computer, information regarding one of the first and second computers to facilitate establishment of a secure connection between the first computer and the second computer. As will be appreciated, then, Aziz already provides for communication between computers on a network, providing secure communication with a relay in a network by between a first computer and a second computer by receiving, at a third computer, information regarding one of the first and second computers to facilitate establishment of a secure connection between the first computer and the second computer.

Applicants respectfully submit that the Office action fails to establish that such a combination of the teachings of these references would meet with success, as is also required. Applicants maintain that Killian and Aziz, in any permissible combination, fail to teach the claimed invention. At best, although Applicants maintain that one of skill in the art would not find such teachings in either reference (and again, aside from using the present Specification as a blueprint, would be forced into undue experimentation to arrive at such a solution), such a combination would at best provide a multi-homed network system in which one or more such connections could be sent via a network connection that provides secure communication with a relay in a network. Regardless, such a system, even if such a combination were shown to be possible, would fail to make obvious the claimed invention, which involves the use of security tokens that are passwords, in the creation of a socket as a result of the receipt of a first connection and a security token.

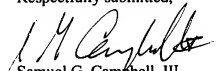
For these reasons, Applicants respectfully submit that the Office Action fails to present a *prima facie* case of obviousness of amended independent claims 107, 120, 131, 140, 165 and 174, and all claims dependent upon them, and that they are in condition for allowance. Applicants therefore request the Examiner's reconsideration of the rejections to those claims.

CONCLUSION

In view of the amendments and remarks set forth herein, the application is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the Examiner is invited to telephone the undersigned at 512-439-5084.

If any extensions of time under 37 C.F.R. § 1.136(a) are required in order for this submission to be considered timely, Applicant hereby petitions for such extensions. Applicant also hereby authorizes that any fees due for such extensions or any other fee associated with this submission, as specified in 37 C.F.R. § 1.16 or § 1.17, be charged to deposit account 502306.

Respectfully submitted,



Samuel G. Campbell, III
Attorney for Applicants
Reg. No. 42,381
Telephone: (512) 439-5084
Facsimile: (512) 439-5099